Amendments To Claims:

This listing of claims replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (currently amended) A method for authenticating data at a server, the method comprising:

a. receiving a data request from a client;

b. retrieving data based on the ~~received~~ data request to obtain retrieved data;

c. ~~upon retrieving the data,~~ formatting the retrieved data in real-time at ~~said~~ the server to create formatted data, wherein the formatted data includes ~~at least one~~ an authenticity key;

d. returning the formatted data to the client; ~~and,~~

e. facilitating authentication of the authenticity key to verify ~~the~~ a source of the formatted ~~data.~~ data;

f. retrieving a preferences key from said server based on said authentication; and,

g. decrypting a preferences file using said preferences key.

2. (original) The method of Claim 1, wherein the formatted data is a web page.

3. (currently amended) The method of Claim 1, further comprising:

a. reading the formatted data at the client;

b. determining if the formatted data includes the ~~at least one~~ authenticity key; and,

~~c. if the formatted data includes the at least one authenticity key;~~

~~d.~~ c. verifying authenticity based on the ~~at least one~~ authenticity key when the formatted data includes the ~~at least one~~ authenticity key.

4. (currently amended) The method of Claim 3, further comprising displaying the formatted data based on the verification of the ~~at least one~~ authenticity key.

5. (currently amended) The method of Claim 4, wherein ~~at least one~~ an authenticity stamp ~~will be~~ is displayed for formatted data that has been successfully verified.

6. (currently amended) The method of Claim 4, wherein ~~one~~ an authenticity stamp ~~will be~~ is displayed for ~~each~~ a graphical image.

7. (currently amended) The method of Claim 4, wherein a non-authenticity stamp ~~will be~~ is displayed for formatted data that has not been successfully ~~been~~ verified.

8. (currently amended) A system for authenticating data, the system comprising:

a. ~~at least one~~ a client;

b. ~~at least one~~ a server;

c. a network, wherein the client and the server communicate via the network; and

d. ~~at least one~~ an authentication server, wherein the ~~said at least one~~ authentication server is in communication with ~~said at least one~~ the server, ~~said~~ the authentication server being configured to insert an authenticity key in real time into the data requested from ~~said~~ the client, thereby facilitating ~~said~~ the client to authenticate the authenticity key to verify the source of ~~the data.~~ the data; and,

e. wherein the client is configured to retrieve a preferences key upon the verification of the source of the data, wherein the preferences key is retrieved from the authentication server and is used to decrypt a preferences file on the client.

9. (currently amended) The system of Claim 8, wherein ~~said at least one~~ the client ~~includes~~ comprises a browser, wherein pages are displayed to a user on a display device on ~~said at least one~~ the client.

10. (currently amended) The system of Claim 8, wherein ~~said at least one~~ the server sends a page including ~~an~~ the authenticity key to ~~said at least one~~ the client.

11. (currently amended) The system of Claim 10, wherein ~~said at least one~~ the client verifies authenticity of the page based on the authenticity key.

12. (currently amended) The system of Claim 11, wherein the page is displayed on ~~said~~ the client, and wherein the display includes an indication of the authenticity of the page.

13. (cancelled).

14. (currently amended) In a computer system for authenticating data at a server, a computer-readable medium holding computer executable instructions for performing a method comprising the steps of:

a. receiving a data request from a client;

b. retrieving data based on the ~~received~~ data request to obtain retrieved data;

c. ~~upon retrieving the data,~~ formatting the retrieved data in real-time at said server to create formatted data, wherein the formatted data includes ~~at least one~~ an authenticity key;

d. returning the formatted data to the client; ~~and,~~

e. facilitating authentication of the authenticity key to verify ~~the~~ a source of the formatted ~~data.~~ data;

f. retrieving a preferences key from said server based on said authentication; and,

g. decrypting a preferences file using said preferences key.

15. (original) The computer system of Claim 14, wherein said formatted data is a web page.

16. (currently amended) The computer system of Claim 14, wherein computer executable instructions further comprise the steps of:

a. reading the formatted data at the client;

b. determining if the formatted data includes the ~~at least one~~ authenticity key; and,

~~c. if the formatted data includes the at least one authenticity key;~~

~~d.~~ c. verifying authenticity based on the ~~at least one~~ authenticity key when the formatted data includes the ~~at least one~~ authenticity key.

17. (currently amended) The computer system of Claim 16, wherein the computer executable instructions further comprise the step of: displaying the formatted data based on the verification of the authenticity.

18. (currently amended) The computer system of Claim 17, wherein ~~at least one~~ an authenticity stamp ~~will be~~ is displayed for formatted data that has been successfully verified.

19. (currently amended) The computer system of Claim 17, wherein ~~at least one~~ a non-authenticity stamp ~~will be~~ is displayed for formatted data that has not been successfully ~~been~~ verified.

20. (currently amended) The method of claim 1, wherein ~~said~~ the receiving and returning steps are implemented via at least one of an internet, interactive television system, broadband system, regular band system, wireless system, radio transmission, landline phone system, and cellular phone system.

21. (currently amended) The method of claim 1, wherein ~~said~~ the step of authenticating the authenticity key to verify the source of the formatted data ~~includes~~ comprises a browser plug-in interfacing with a MIME type to authenticate a ~~the formatted data~~ private key included in the formatted data.

22. (currently amended) The system of claim 8, wherein said authentication server is configured to authenticate a user ID and a password.

23. (currently amended) The system of claim 8, wherein said authentication server is configured to sign ~~the~~ a web page.

24. (currently amended) A method for authenticating data at a server, the method comprising:

receiving a data request from a client;

retrieving data based on the ~~received~~ data request to obtain retrieved data;

~~upon retrieving the data,~~ determining if said data includes a code which requires ~~said~~ the data to be authenticated;

formatting the retrieved data in real-time at said server to create formatted data, wherein the formatted data includes ~~at least one~~ an authenticity key;

returning the formatted data to the client; ~~and,~~

facilitating authentication of the authenticity key to verify the source of the formatted ~~data.~~ data; and,

retrieving a preferences key based on the authentication, wherein the preferences key is retrieved from the server.

25. (currently amended) The method of claim 24, further comprising:

~~decrypting a preferences key;~~

~~decrypting a preferences file using said preferences key;~~

obtaining instructions within ~~said~~ the preferences file; and,

inserting a visual signature into ~~said~~ the formatted data based on ~~said~~ the instructions stored in ~~said~~ the preferences file.

26. (currently amended) The method of claim 24 further comprising:

decrypting a the preferences key using a master preferences key;

~~decrypting a preferences file using said preferences key;~~

obtaining instructions within ~~said~~ the preferences file; and,

inserting a visual signature into ~~said~~ the formatted data based on ~~said~~ the instructions stored in ~~said~~ the preferences filc.

27. (currently amended) The method of claim 1, further comprising:

~~decrypting a preferences key;~~

~~decrypting a preferences file using said preferences key;~~

obtaining instructions within ~~said~~ the preferences file; and, inserting a visual signature into ~~said~~ the formatted data based on ~~said~~ the instructions stored in ~~said~~ the preferences file.

28. (currently amended) The method of claim 1, further comprising:

decrypting ~~a~~ the preferences key using a master preferences key;

~~decrypting a preferences file using said preferences key;~~

obtaining instructions within ~~said~~ the preferences file; and,

inserting a visual signature into ~~said~~ the formatted data based on ~~said~~ the instructions stored in ~~said~~ the preferences file.

29. (New) A method for authenticating data at a server, the method comprising:

receiving a data request from a client;

retrieving data based on the data request to obtain retrieved data;

formatting the retrieved data in real-time at the server to create formatted data, wherein the formatted data includes an authenticity key;

returning the formatted data to the client; and,

facilitating authentication of the authenticity key to verify a source of the formatted data;

decrypting a preferences key;

decrypting a preferences file using the preferences key;

obtaining instructions within the preferences file; and,

inserting a visual signature into the formatted data based on the instructions stored in the preferences file.

30. (New) A method for authenticating data at a server, the method comprising:

receiving a data request from a client;

retrieving data based on the data request to obtain retrieved data;

determining if the data includes a code which requires the data to be authenticated;

formatting the retrieved data in real-time at said server to create formatted data, wherein the formatted data includes an authenticity key;

returning the formatted data to the client;

facilitating authentication of the authenticity key to verify the source of the formatted data;

decrypting a preferences key;

decrypting a preferences file using the preferences key;

obtaining instructions within the preferences file; and,

inserting a visual signature into the formatted data based on the instructions stored in the preferences file.